Patent
Attorney's Docket No. 030675-054

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Masaki OMATA	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Examiner: Unassigned
	)	
Filed: June 5, 2001	)	
	)	
For: USER AUTHENTICATION SYSTEM	)	
	)	
	)	
	)	
	)	

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed:

Japanese Patent Application No. 2000-209857

Filed: July 11, 2000

In support of this claim, enclosed is a certified copy of said prior foreign application. Said prior foreign application was referred to in the oath or declaration. Acknowledgment of receipt of the certified copy is requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: June 5, 2001

By: _____
Platon N. Mandros
Registration No. 22,124

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ７月１１日

出 願 番 号
Application Number: 特願２０００－２０９８５７

出 願 人
Applicant (s): 三菱電機株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 １月 ５日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２０００－３１１０２００

Translation of Priority Certificate

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: July 11, 2000

Application Number: Patent Application
No. 2000-209857

Applicant(s): MITSUBISHI DENKI KABUSHIKI KAISHA

January 5, 2001

Commissioner, Kozo Oikawa
Patent Office

Priority Certificate No. 2000-3110200

【書類名】　特許願
【整理番号】　525497JP01
【提出日】　平成12年 7月11日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 17/60
【発明者】
　【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
　【氏名】　小俣　正樹
【特許出願人】
　【識別番号】　000006013
　【氏名又は名称】　三菱電機株式会社
【代理人】
　【識別番号】　100075258
　【弁理士】
　【氏名又は名称】　吉田　研二
【選任した代理人】
　【識別番号】　100081503
　【弁理士】
　【氏名又は名称】　金山　敏彦
【選任した代理人】
　【識別番号】　100096976
　【弁理士】
　【氏名又は名称】　石田　純
【手数料の表示】
　【予納台帳番号】　001753
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　ユーザ認証システム

【特許請求の範囲】

【請求項１】　音声入力機能付き通信端末装置からのログインを許可する際に、ユーザを一意に特定するユーザ識別情報及びそのユーザ識別情報に対応したパスワードに基づくユーザ認証を行うユーザ認証システムにおいて、

ユーザ識別情報と、当該ユーザが当該ユーザ識別情報を発声して得られる声紋情報とを対応付けして格納するユーザ認証データベースを有し、データ通信網を介して前記音声入力機能付き通信端末装置から送られてきたコード形式のユーザ識別情報に基づき前記ユーザ認証データベースを検索することにより特定される声紋情報と、電話回線網を介して前記音声入力機能付き通信端末装置から送られてきた音声形式によるユーザ識別情報とに基づき照合することによってユーザ認証を行うことを特徴とするユーザ認証システム。

【請求項２】　ユーザを一意に特定するユーザ識別情報及びそのユーザ識別情報に対応したパスワードに基づくユーザ認証後に使用を許可するシステムにログイン可能な音声入力機能付き通信端末装置と、

ユーザ識別情報と、当該ユーザが当該ユーザ識別情報を発声して得られる声紋情報とを対応付けして格納するユーザ認証データベースと、

データ通信網を介して前記音声入力機能付き通信端末装置からコード形式ユーザ識別情報が送られてきたときにワンタイム識別情報を生成し、その生成したワンタイム識別情報を、データ通信網を介して前記音声入力機能付き通信端末装置へ返信すると共にそのワンタイム識別情報をパスワードとして指定したログインを不可の状態にして当該ユーザ識別情報に対応付けして前記ユーザ認証データベースへ書き込むワンタイム識別情報管理手段と、

電話回線網を介して前記音声入力機能付き通信端末装置から音声形式ユーザ識別情報が送られてきたときに、前記ユーザ認証データベースを参照することによって音声形式ユーザ識別情報に基づき声紋認証を行い、認証にパスしたときには前記ユーザ認証データベースに書き込まれている当該ワンタイム識別情報でのログインを可能状態に変更するユーザ認証処理手段と、

を有し、

前記音声入力機能付き通信端末装置は、

自通信端末装置の識別情報あるいは自通信端末装置を専用するユーザの識別情報をコード形式ユーザ識別情報として前記ワンタイム識別情報管理手段へ送信するコード形式ユーザ識別情報送信処理手段と、

ユーザにより音声入力されたユーザ識別情報を受け付けて音声形式ユーザ識別情報として前記ユーザ認証処理手段へ送信する音声形式ユーザ識別情報送信処理手段と、

前記ユーザ認証処理手段によるユーザ認証完了後に、前記ワンタイム識別情報管理手段から送られてきたワンタイム識別情報を用いてシステムに自動ログインする自動ログイン処理手段と、

を有することを特徴とするユーザ認証システム。

【請求項３】　前記ユーザ認証処理手段は、

電話回線網を介して前記音声入力機能付き通信端末装置から送られてきた音声形式ユーザ識別情報に対して音声認識処理を行うことによってコード形式でのユーザ識別情報を得る音声認識処理部と、

前記音声認識処理部により取得されたユーザ識別情報に基づいて前記ユーザ認証データベースを検索することにより特定した声紋情報と、前記音声入力機能付き通信端末装置から送られてきた音声形式ユーザ識別情報とに基づき照合を行うことで声紋認証を行う声紋認証処理部と、

有することを特徴とする請求項２記載のユーザ認証システム。

【請求項４】　前記コード形式ユーザ識別情報送信処理手段は、データ通信網を介してシステムから送られてきたログイン画面を前記音声入力機能付き通信端末装置に画面表示し、そのログイン画面から入力されたユーザ名をコード形式ユーザ識別情報として前記ワンタイム識別情報管理手段へ送信することを特徴とする請求項２記載のユーザ認証システム。

【請求項５】　前記音声形式ユーザ識別情報送信処理手段は、前記ワンタイム識別情報管理手段からデータ通信網を介してワンタイム識別情報が送られてきた後、前記ユーザ認証処理手段から電話回線網を介して送られてきた音声ガイダ

ンスに従いユーザにより入力された音声を音声形式ユーザ識別情報として前記ユーザ認証処理手段へ送信することを特徴とする請求項２記載のユーザ認証システム。

【請求項６】　前記音声入力機能付き通信端末装置からのユーザログインが完了した時点で、対応するワンタイム識別情報を前記ユーザ認証データベースから自動消去するワンタイム識別情報削除処理手段を有することを特徴とする請求項２記載のユーザ認証システム。

【請求項７】　前記音声入力機能付き通信端末装置は、インターネット機能付き携帯電話であることを特徴とする請求項１又は２記載のユーザ認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はユーザ認証システム、特にセキュリティ強度を維持しつつ、ログインに要するユーザ負荷の軽減を図るユーザ認証システムに関する。

【０００２】

【従来の技術】

ユーザ認証後に使用が許可されるシステムにおいてユーザ認証を行うための代表的な手法として、端末装置からユーザ名とパスワードを入力させる方法がある。近年では、ｉモード（商標）などと呼ばれるインターネット機能等を搭載したインターネット機能付き携帯電話（以下、単に「携帯電話」とも称する）の普及に伴い、社員が所持する携帯電話から企業内コンピュータへログインできるように社内システムを構築している企業は少なくない。但し、この場合、なりすましと呼ばれる第三者による社内システムへの不正侵入を防止するためにもセキュリティを確保する必要がある。セキュリティの確保のために、例えば、パスワードを長くしたり、大小英文字を混在させたりするなどパスワードを複雑にすることで、場当たり的な英数文字の組合せ入力によるパスワード一致を発生しにくくしている。また、有効期間を短くするなどして見破られたパスワードの再利用を防止したりしている。

【０００３】

【発明が解決しようとする課題】

しかしながら、パスワードを複雑にした場合、特に英数文字を混在させた場合、数字キー以外のキーと組み合わせたモード切替操作を頻繁に行いながら携帯電話からパスワード入力をしなくてはならず、パスワード指定が極めて面倒である。機種によっては多少異なるかもしれないが、例えば、“9v”という２文字を携帯電話のキーから入力するときには、[9] [ﾓｰﾄﾞ] [ﾓｰﾄﾞ] [ﾓｰﾄﾞ] [ﾓｰﾄﾞ] [8] [8] [8]（[]は１回のキー操作を示す）という８回ものキー操作が必要となる。これを通常指定するパスワード長に当てはめると、携帯電話からのパスワード指定が極めて面倒なことが容易に把握できる。

【０００４】

本発明は以上のような問題を解決するためになされたものであり、その目的は、高いセキュリティ性を維持しつつユーザにかかる入力負荷を軽減させることのできるユーザ認証システムを提供することにある。

【０００５】

【課題を解決するための手段】

以上のような目的を達成するために、本発明に係るユーザ認証システムは、音声入力機能付き通信端末装置からのログインを許可する際に、ユーザを一意に特定するユーザ識別情報及びそのユーザ識別情報に対応したパスワードに基づくユーザ認証を行うユーザ認証システムにおいて、ユーザ識別情報と、当該ユーザが当該ユーザ識別情報を発声して得られる声紋情報とを対応付けして格納するユーザ認証データベースを有し、データ通信網を介して前記音声入力機能付き通信端末装置から送られてきたコード形式のユーザ識別情報に基づき前記ユーザ認証データベースを検索することにより特定される声紋情報と、電話回線網を介して前記音声入力機能付き通信端末装置から送られてきた音声形式によるユーザ識別情報とに基づき照合することによってユーザ認証を行うものである。

【０００６】

また、他の発明に係るユーザ認証システムは、ユーザを一意に特定するユーザ識別情報及びそのユーザ識別情報に対応したパスワードに基づくユーザ認証後に

使用を許可するシステムにログイン可能な音声入力機能付き通信端末装置と、ユーザ識別情報と、当該ユーザが当該ユーザ識別情報を発声して得られる声紋情報とを対応付けして格納するユーザ認証データベースと、データ通信網を介して前記音声入力機能付き通信端末装置からコード形式ユーザ識別情報が送られてきたときにワンタイム識別情報を生成し、その生成したワンタイム識別情報を、データ通信網を介して前記音声入力機能付き通信端末装置へ返信すると共にそのワンタイム識別情報をパスワードとして指定したログインを不可の状態にして当該ユーザ識別情報に対応付けして前記ユーザ認証データベースへ書き込むワンタイム識別情報管理手段と、電話回線網を介して前記音声入力機能付き通信端末装置から音声形式ユーザ識別情報が送られてきたときに、前記ユーザ認証データベースを参照することによって音声形式ユーザ識別情報に基づき声紋認証を行い、認証にパスしたときには前記ユーザ認証データベースに書き込まれている当該ワンタイム識別情報でのログインを可能状態に変更するユーザ認証処理手段とを有し、前記音声入力機能付き通信端末装置は、自通信端末装置の識別情報あるいは自通信端末装置を専用するユーザの識別情報をコード形式ユーザ識別情報として前記ワンタイム識別情報管理手段へ送信するコード形式ユーザ識別情報送信処理手段と、ユーザにより音声入力されたユーザ識別情報を受け付けて音声形式ユーザ識別情報として前記ユーザ認証処理手段へ送信する音声形式ユーザ識別情報送信処理手段と、前記ユーザ認証処理手段によるユーザ認証完了後に、前記ワンタイム識別情報管理手段から送られてきたワンタイム識別情報を用いてシステムに自動ログインする自動ログイン処理手段とを有するものである。

【０００７】

また、前記ユーザ認証処理手段は電話回線網を介して前記音声入力機能付き通信端末装置から送られてきた音声形式ユーザ識別情報に対して音声認識処理を行うことによってコード形式でのユーザ識別情報を得る音声認識処理部と、前記音声認識処理部により取得されたユーザ識別情報に基づいて前記ユーザ認証データベースを検索することにより特定した声紋情報と、前記音声入力機能付き通信端末装置から送られてきた音声形式ユーザ識別情報とに基づき照合を行うことで声紋認証を行う声紋認証処理部と有するものである。

【０００８】

あるいは、前記コード形式ユーザ識別情報送信処理手段は、データ通信網を介してシステムから送られてきたログイン画面を前記音声入力機能付き通信端末装置に画面表示し、そのログイン画面から入力されたユーザ名をコード形式ユーザ識別情報として前記ワンタイム識別情報管理手段へ送信するものである。

【０００９】

あるいは、前記音声形式ユーザ識別情報送信処理手段は、前記ワンタイム識別情報管理手段からデータ通信網を介してワンタイム識別情報が送られてきた後、前記ユーザ認証処理手段から電話回線網を介して送られてきた音声ガイダンスに従いユーザにより入力された音声を音声形式ユーザ識別情報として前記ユーザ認証処理手段へ送信するものである。

【００１０】

あるいは、前記音声入力機能付き通信端末装置からのユーザログインが完了した時点で、対応するワンタイム識別情報を前記ユーザ認証データベースから自動消去するワンタイム識別情報削除処理手段を有するものである。

【００１１】

あるいは、前記音声入力機能付き通信端末装置は、インターネット機能付き携帯電話であるものとする。

【００１２】

【発明の実施の形態】

以下、図面に基づいて、本発明の好適な実施の形態について説明する。なお、本実施の形態では、本発明に係るユーザ認証システムを社内システムに適用した場合を例にして説明する。

【００１３】

図１は、本発明に係るユーザ認証システムの一実施の形態を示したシステム構成図である。インターネット機能付きの携帯電話１のユーザは、携帯電話メーカのパケット通信網を介して回線接続された相手先と対話ができるのみならず、インターネットに接続してサービス提供業者が提供する各種サービスの提供を受けることができる。このとき、通常の会話を行う際には、電話番号で指定した相手

先との間に電話回線網２を介して回線が確立され、インターネット等を利用する際には、アドレス指定をして特定したログイン先との間にデータ通信網３を介して回線が確立される。なお、本実施の形態において、インターネットはデータ通信網３に包含され、また、携帯電話メーカのパケット通信網はデータ通信網３及び電話回線網２の双方の一部を構成するため、図１においては便宜的に図示していない。

【００１４】

本実施の形態における社内システムは、Ｗｅｂサーバ４、データベースサーバ５、ＣＴＩ(Computer Telephony Integration)サーバ６及び認証サーバ７をＬＡＮ８で接続することによって構築されている。Ｗｅｂサーバ４は、携帯電話１からの要求に応じてサービスを提供するサーバであり、データ通信網３を介して携帯電話１とデータ通信を行う。データベースサーバ５は、ユーザ認証データベース９を管理するサーバである。ＣＴＩサーバ６は、コンピュータと電話とを統合させたサーバであり、電話回線網２を介して送られてくる携帯電話１からの音声を認識する機能を有している。認証サーバ７は、声紋認証を行うためのサーバである。

【００１５】

ユーザ認証データベース９には、社員ＩＤに、当該ユーザが当該社員ＩＤを発声したときの声紋情報が対応付けされて予め格納されている。本実施の形態における社員ＩＤは、社内システムに登録されたユーザを識別するためのユーザ識別情報に相当する。携帯電話１を用いて社外から社内システムにアクセスするためには、その社員の声紋情報を予め登録しておく必要がある。詳細は後述するが、社員ＩＤには、更に認証処理において生成／消去されるワンタイムＩＤが対応付けして格納される。ワンタイムＩＤというのは、一度きりの使用が認められているパスワードである。

【００１６】

この構成において本実施の形態に含まれるワンタイムＩＤ管理部１０、ユーザ認証処理部１１及びワンタイムＩＤ削除処理部１２の各機能ブロックは、図１に示したように各サーバ４～７をまたいで配設される。つまり、各処理機能は、モ

ジュールを各サーバに分散配置して実現され、以下のように作用する。すなわち、ワンタイムＩＤ管理部１０は、データ通信網３を介して携帯電話１からコード形式の社員ＩＤが送られてきたときにワンタイムＩＤ生成し、その生成したワンタイムＩＤを、データ通信網３を介して携帯電話１へ返信すると共にそのワンタイムＩＤを指定したログインを不可の状態にして当該社員ＩＤに対応付けしてユーザ認証データベース９へ書き込むが、この処理機能のうちデータベースアクセス部分の機能モジュールがデータベースサーバ５に設けられている。ユーザ認証処理部１１は、ＣＴＩサーバ６に配設される音声認識処理部１３と認証サーバ７に配設される声紋認証処理部１４とを有している。音声認識処理部１３は、電話回線網２を介して携帯電話１から送られてきた音声形式の社員ＩＤに対して音声認識処理を行うことによってコード形式での社員ＩＤを得る。声紋認証処理部１４は、音声認識処理部１３により取得された社員ＩＤに基づいてユーザ認証データベース９を検索することにより声紋情報を特定し、その特定した声紋情報と携帯電話１から送られてきた音声形式の社員ＩＤとに基づき照合を行うことで声紋認証を行う。そして、ユーザ認証処理部１１は、認証にパスしたときにはユーザ認証データベース９に書き込まれているワンタイムＩＤでのログインを可能状態に変更する。ワンタイムＩＤ削除処理部１２は、携帯電話１からのユーザログインが完了した時点で、対応するワンタイムＩＤをユーザ認証データベース９から自動消去する。

【００１７】

一方、本実施の形態における携帯電話１には、コード形式の社員ＩＤをＣＴＩサーバ６に配設されているワンタイムＩＤ管理部１０へ送信するコード形式社員ＩＤ送信処理部１５と、ユーザにより音声入力された社員ＩＤを音声認識処理部１３へ送信する音声形式社員ＩＤ送信処理部１６と、ユーザ認証完了後にワンタイムＩＤ管理部１０から送られてきたワンタイムＩＤを用いてシステムに自動ログインする自動ログイン処理部１７とを有している。なお、本実施の形態のように音声入力機能付き通信端末装置が携帯電話の場合、図１に明示するまでもなく、音声形式社員ＩＤ送信処理部１６は通常の電話機能として当然持っている処理機能であり、携帯電話がインターネット機能付きであればコード形式社員ＩＤ送

信処理部１５も当然持っている処理機能である。なお、携帯電話１は、その他にも画面表示等種々の機能を有しているが、それら通常保有している機能は本実施の形態の要旨でないため説明は省略する。各サーバ４～７においても同様である。

【００１８】

以上の構成を有する本実施の形態において特徴的なことは、声紋認証機能とワンタイムパスワード発行機能とを有機的に結合させたことにより、携帯電話１からパスワード入力のためのキー操作をさせずに社内システムにログインできるようにしたことである。本実施の形態においては、声紋情報及びワンタイムパスワードを有効に利用したことでセキュリティ強度を維持しつつユーザにかかる入力負荷を軽減することができる。

【００１９】

次に、本実施の形態においてユーザ（社員）が携帯電話１から社内システムにログインしようとしたときにおける動作について図２及び図３に示したフローチャート及び図４に示したユーザシーンを用いて説明する。

【００２０】

ユーザが携帯電話１のインターネット機能を利用してＷｅｂサーバ４へアクセスすると、携帯電話１は、Ｗｅｂサーバ４からダウンロードされてきたログイン画面を表示する（ステップ１０１）。このログイン画面の例を図４（ａ）に示す。なお、このときはまだ社内システムにログインされていない状態である。ユーザは、このログイン画面から自分の社員ＩＤを入力し、ＯＫボタンを押下する。携帯電話１は、入力された社員ＩＤを受け付けると（ステップ１０２）、コード形式社員ＩＤ送信処理部１５に社員ＩＤをＷｅｂサーバ４へ送信させる。

【００２１】

Ｗｅｂサーバ４では、送られてきた社員ＩＤがユーザ認証データベース９に登録されているかをデータベースサーバ５経由で確認し、もし、登録されていなければ、ログイン画面を携帯電話１に再度表示する（ステップ１０３，１０１）。一方、登録されていたときにはワンタイムＩＤを生成する（ステップ１０４）。そして、生成したワンタイムＩＤをパスワードとして指定したログインを不可の

状態にして当該社員ＩＤに対応付けしてユーザ認証データベース９へ書き込む（ステップ１０５）。更に、当該社員ＩＤをユーザ名に指定したログインを不可の状態に変更する（ステップ１０６）。社員ＩＤ及びワンタイムＩＤの各ログイン可／不可状態は、例えばフラグ情報などによりユーザ認証データベース９で保持するようにすればよい。ワンタイムＩＤをパスワードに指定したログインを不可の状態にすることによってユーザ認証前においてそのワンタイムＩＤによる不正なログインを防止することができる。また、本実施の形態における社員システムでは、同一ユーザに複数ログインさせないように運用しているので、社員ＩＤをユーザ名に指定したログインを不可の状態にすることによって不正なログインを防止することができる。Ｗｅｂサーバ４は、その後、生成したワンタイムＩＤを携帯電話１へ返信すると共に認証画面を送信する。

【００２２】

携帯電話１は、Ｗｅｂサーバ４から送られてきたワンタイムＩＤを内部で一時保持すると共に認証画面を表示する（ステップ１０７）。なお、ワンタイムＩＤは画面表示しない。ユーザは、図４（ｂ）に示した認証画面に表示されたガイダンスに従い、画面表示されたＣＴＩサーバ６の電話番号をキー入力する。携帯電話１は、ユーザのキー入力に応じてＣＴＩサーバ６にダイヤル発信して回線接続する。そして、ユーザ認証処理部１１による声紋照合処理が開始される（ステップ１０８，１０９）。この声紋照合処理の詳細を図３に示す。

【００２３】

ＣＴＩサーバ６と携帯電話１との回線接続後、ＣＴＩサーバ６は、社員ＩＤを発生することを促す音声ガイダンスを携帯電話１に送る（ステップ２０１）。そして、ユーザは、ＣＴＩサーバ６からの音声ガイダンスに従い、社員ＩＤを発声する。つまり、ユーザは、複雑でかつ長い文字列のパスワードをキー入力する代わりに社員ＩＤを発声することになる。ＣＴＩサーバ６の音声認識処理部１３は、ユーザにより発生された音声に対して音声認識処理を施してコード形式の社員ＩＤを得る（ステップ２０２）。

【００２４】

そして、認証サーバ７の声紋認証処理部１４は、音声認識処理部１３により取

得された社員ＩＤ（コード形式）に基づいてユーザ認証データベース９を検索することにより社員ＩＤが登録されているか確認する（ステップ２０４）。本実施の形態では、社員ＩＤを発声させ、それを音声認識処理することで社員ＩＤを一意に特定することができるので、データ登録数が膨大であってもユーザ認証データベース９の検索処理を極めて迅速に行うことができる。もし、音声から得られた社員ＩＤが登録されていないようであれば、音声ガイダンスを流してユーザに社員ＩＤを再度発声してもらう（ステップ２０３，２０１）。ここで、社員ＩＤが登録されていることが確認できると、その社員ＩＤにより対応した声紋情報と、携帯電話１から送られてきた音声から得られる声紋との照合を行う（ステップ２０４）。照合した結果、一致したときには正しいユーザであると判断して、ユーザ認証データベース９に登録されている当該社員ＩＤに対応したワンタイムＩＤのログインを可能な状態に変更する（ステップ２０５，２０６）。なお、当該社員ＩＤでのログインは不可の状態のままである。

【００２５】

ＣＴＩサーバ６は、認証できたか否かの旨の音声ガイダンスをユーザに対して流した後、電話回線網２を介しての回線を切断することでユーザ認証処理を終了させる（ステップ２０７）。

【００２６】

ユーザは、認証されたことをＣＴＩサーバ６からの音声メッセージにより確認すると、認証画面のガイダンスに従いＯＫボタンを押下する（ステップ１０８）。これにより、自動ログイン処理部１７は、内部に保持しておいたワンタイムＩＤをＷｅｂサーバ４に送信することでシステムに自動ログインする。ユーザが正当に認証された後であれば、声紋照合処理のステップ２０６においてワンタイムＩＤでのログインが可能な状態に変更されているので、ログインすることができる。もし、ユーザ認証される前にＯＫボタンが押下されたとしてもワンタイムＩＤでのログインは不可の状態のままなのでログインをすることはできない。

【００２７】

Ｗｅｂサーバ４は、ユーザログインを確認すると、ワンタイムＩＤ削除処理部１２によって、当該ユーザに対応したワンタイムＩＤをユーザ認証データベース

９から即座に自動消去させる（ステップ１１１）。これにより、そのワンタイムＩＤを再利用した不正ログインを未然に防止する。そして、図４（ｃ）に例示したような社内システムのメイン画面を携帯電話１に画面表示させる（ステップ１１２）。なお、本実施の形態における社員システムでは、同一ユーザによる複数ログインを禁止しているので、当該社員ＩＤでのログインは不可の状態のままである。

【００２８】

ユーザが社内システムの利用を終了し、ログアウトすると、ＣＴＩサーバ６は、データベースサーバ５に当該社員ＩＤでのログインを可能な状態に変更させる（ステップ１１３）。

【００２９】

パスワードを指定した一般的なユーザ認証処理では、ユーザ名や本実施の形態の社員ＩＤのようなユーザ識別情報と（ワンタイム）パスワードとの組合せによりユーザ照合を行う。このうちユーザ識別情報というのは、社員番号や人名、あるいはこれらの組合せなどから構成される文字列であって、ある程度の規則性があるため見破られやすい。そこで、パスワードを指定することでセキュリティの維持を図るようにしているが、セキュリティ強度を高めるためにパスワードを複雑にする必要があるが、特に携帯電話等設けるキーの数が制限されるような機器ではその指定が特に面倒になってしまう。

【００３０】

そこで、本実施の形態では、必ず指定しなければならないユーザ識別情報は他人に知られても良いことを前提に簡単な文字列で構成可能とし、その一方でユーザに入力指定させることのない、かつ第三者に簡単には見破られない複雑なワンタイムＩＤをユーザ識別情報に対応して設定し、かつパスワード指定の代わりに音声入力させ声紋認証を行うようにしたことで、ユーザは入力が簡単なユーザ識別情報を指定するだけでログインすることができる。

【００３１】

本実施の形態によれば、以上のようにワンタイムＩＤを用いることでセキュリティを維持することができ、声紋によるユーザ認証を利用することによって複雑

なパスワード指定をユーザにさせずにすむので、ログインの際に要するユーザ入力負荷を軽減することができる。

【００３２】

また、本実施の形態では、社員ＩＤでログインさせるのではなくワンタイムＩＤでログインさせるようにした。これは、比較的簡単な文字列で構成される社員ＩＤをそのまま用いると、社員ＩＤによる声紋認証（ステップ２０５）が完了してからワンタイムＩＤによるログインまで（ステップ１０８）の時間の隙間に第三者が社員ＩＤを用いてログインできる可能性があるからである。複雑な指定が可能なワンタイムＩＤを用いれば、上記隙間の時間内に第三者がワンタイムＩＤを特定できる可能性が極めて低く、現実的には不可能と考えられる。更に、本実施の形態によれば、ワンタイムＩＤを用いたログイン可／不可の状態を設定、保持するようにしたので、仮にワンタイムＩＤを見破ったとしても不当な時間帯（つまり、ログイン不可状態が設定されている時間帯）にそのワンタイムＩＤを用いてログインすることはできない。

【００３３】

なお、本実施の形態では、ユーザ識別情報として社員ＩＤを用いたが、ユーザが特定できれば、例えば、そのユーザが固有して用いる会員番号や電話番号でもよい。更に、ユーザが特定の携帯電話のみを使用する場合は、携帯電話に割り当てられている固有な情報をユーザ識別情報として使用することができる。この場合、ユーザはその携帯電話１の識別情報を音声により発声さえすれば何らキー入力することなくログインできることになる。

【００３４】

また、本実施の形態においては、音声入力機能付き通信端末装置としてインターネット機能付きの携帯電話１を例にして説明したが、例えば通信機能及び音声入力機能を搭載したテレフォニー端末装置やパーソナルコンピュータなどの情報端末機器でも通信機能及び音声入力機能を搭載させることで本発明を適用することができる。

【００３５】

【発明の効果】

本発明によれば、ユーザ識別情報とは別個に用意しかつユーザに入力指定させる必要のないワンタイム識別情報を設定し、かつ声紋照合によるユーザ認証を行うようにしたので、セキュリティの維持を図りつつログインの際に要するユーザ入力負荷を軽減させることができる。

【００３６】

特に、本発明においては、ログイン要求に応じて生成したワンタイム識別情報を用いてのログイン可／不可の状態を設定、保持するようにしたので、ワンタイム識別情報の生成から正当ユーザによる当該ワンタイム識別情報を用いたログイン処理終了までのわずかな時間の隙間における不正ログインを防止することができる。

【００３７】

また、ユーザログインが完了した時点で、対応するワンタイム識別情報をユーザ認証データベースから自動消去するようにしたので、ワンタイム識別情報を再利用した不正ログインを未然に防止することができる。

【図面の簡単な説明】

【図１】　本発明に係るユーザ認証システムの一実施の形態を示したシステム構成図である。

【図２】　本実施の形態におけるユーザ認証処理を示したフローチャートである。

【図３】　本実施の形態における声紋照合処理を示したフローチャートである。

【図４】　本実施の形態においてユーザ認証時におけるユーザシーンを示した概念図である。

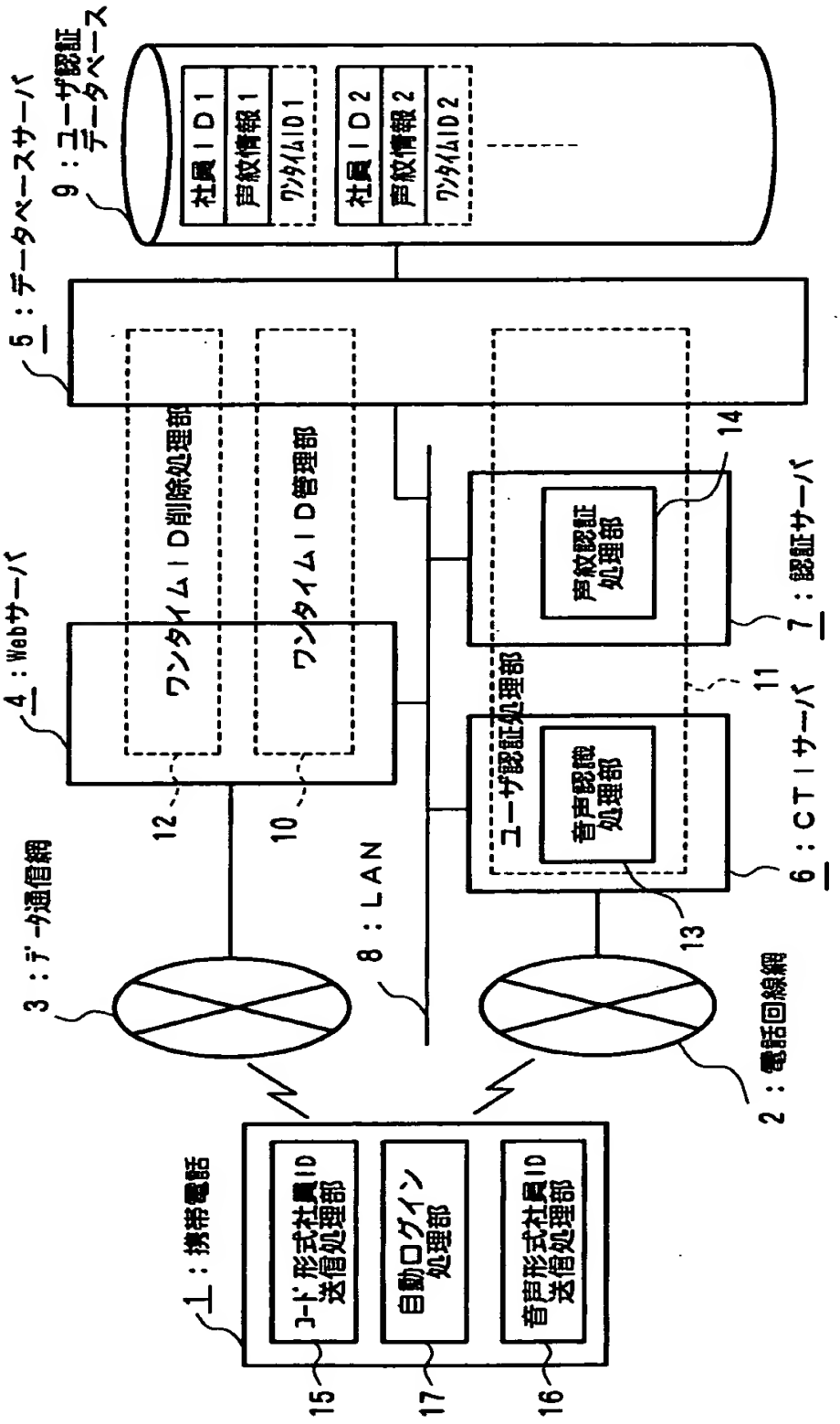
【符号の説明】

１　（インターネット機能付き）携帯電話、２　電話回線網、３　データ通信網、４　Ｗｅｂサーバ、５　データベースサーバ、６　ＣＴＩサーバ、７　認証サーバ、８　ＬＡＮ、９　ユーザ認証データベース、１０　ワンタイムＩＤ管理部、１１　ユーザ認証処理部、１２　ワンタイムＩＤ削除処理部、１３　音声認識処理部、１４　声紋認証処理部、１５　コード形式社員ＩＤ送信処理部、１６

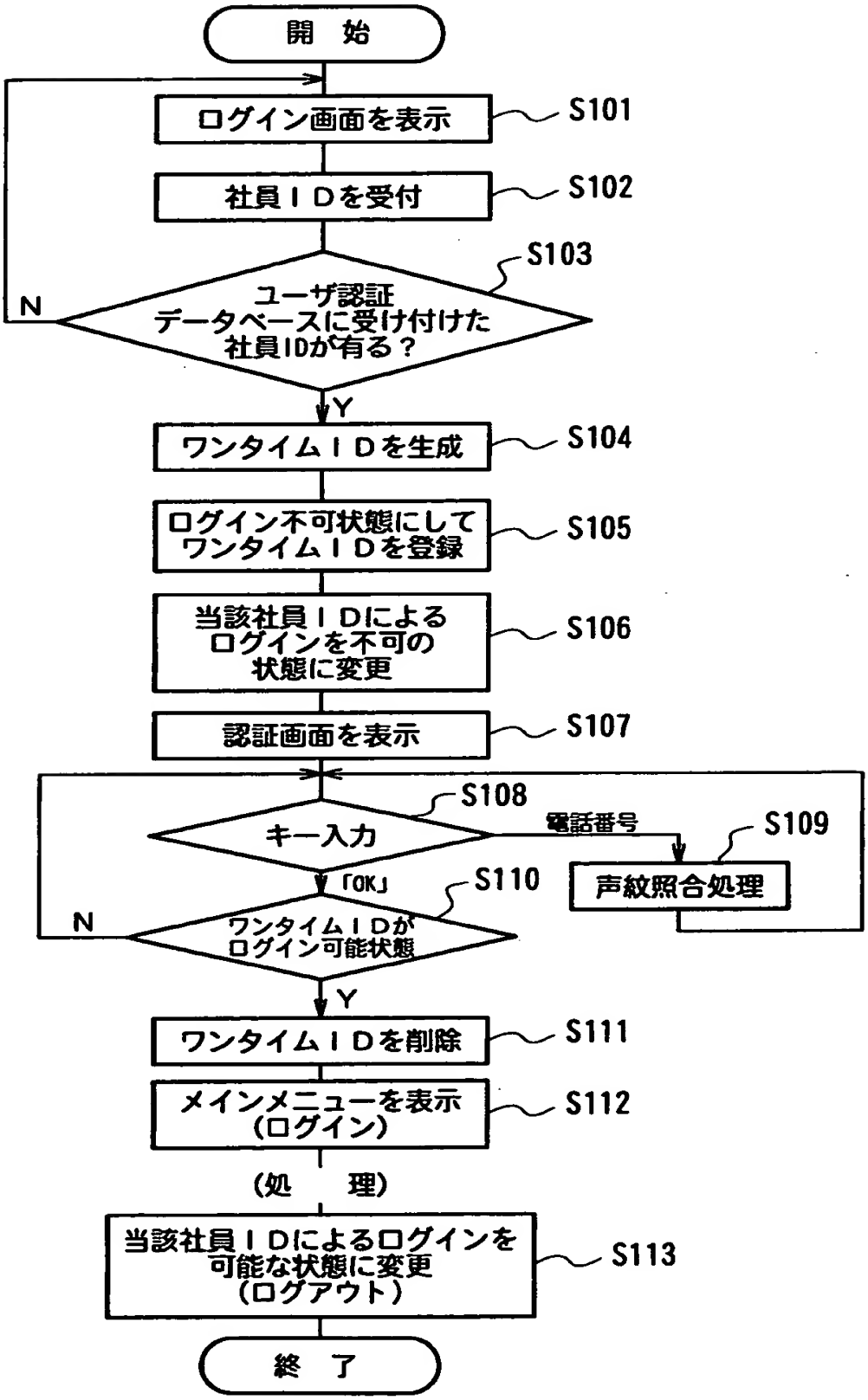
音声形式社員ＩＤ送信処理部、１７　自動ログイン処理部。

【書類名】　　図面

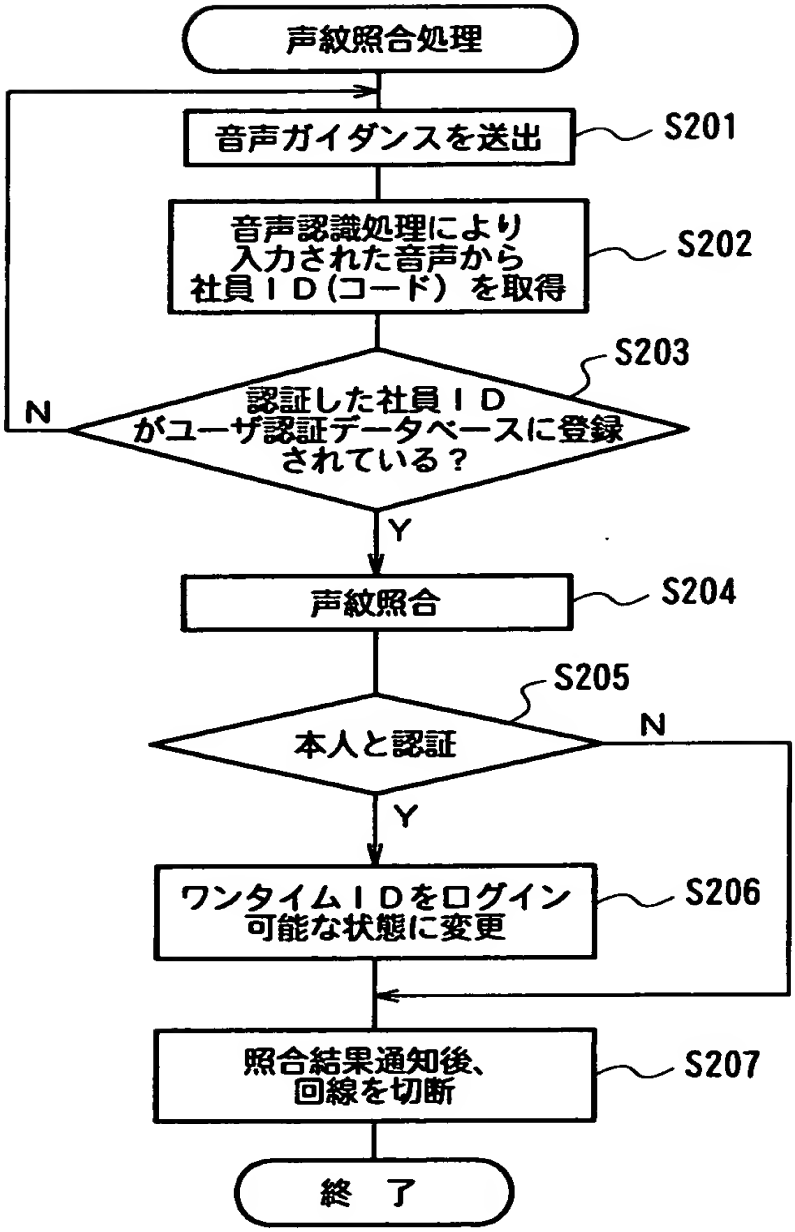
【図１】


1：携帯電話
2：電話回線網
3：データ通信網
4：Webサーバ
5：データベースサーバ
6：CTIサーバ
7：認証サーバ
8：LAN
9：ユーザ認証データベース
10
11
12
13
14
15
16
17
社員ID1
声紋情報1
ワンタイムID1
社員ID2
声紋情報2
ワンタイムID2
ワンタイムID削除処理部
ワンタイムID管理部
ユーザ認証処理部
声紋認証処理部
音声認識処理部
ｺｰﾄﾞ形式社員ID送信処理部
自動ログイン処理部
音声形式社員ID送信処理部

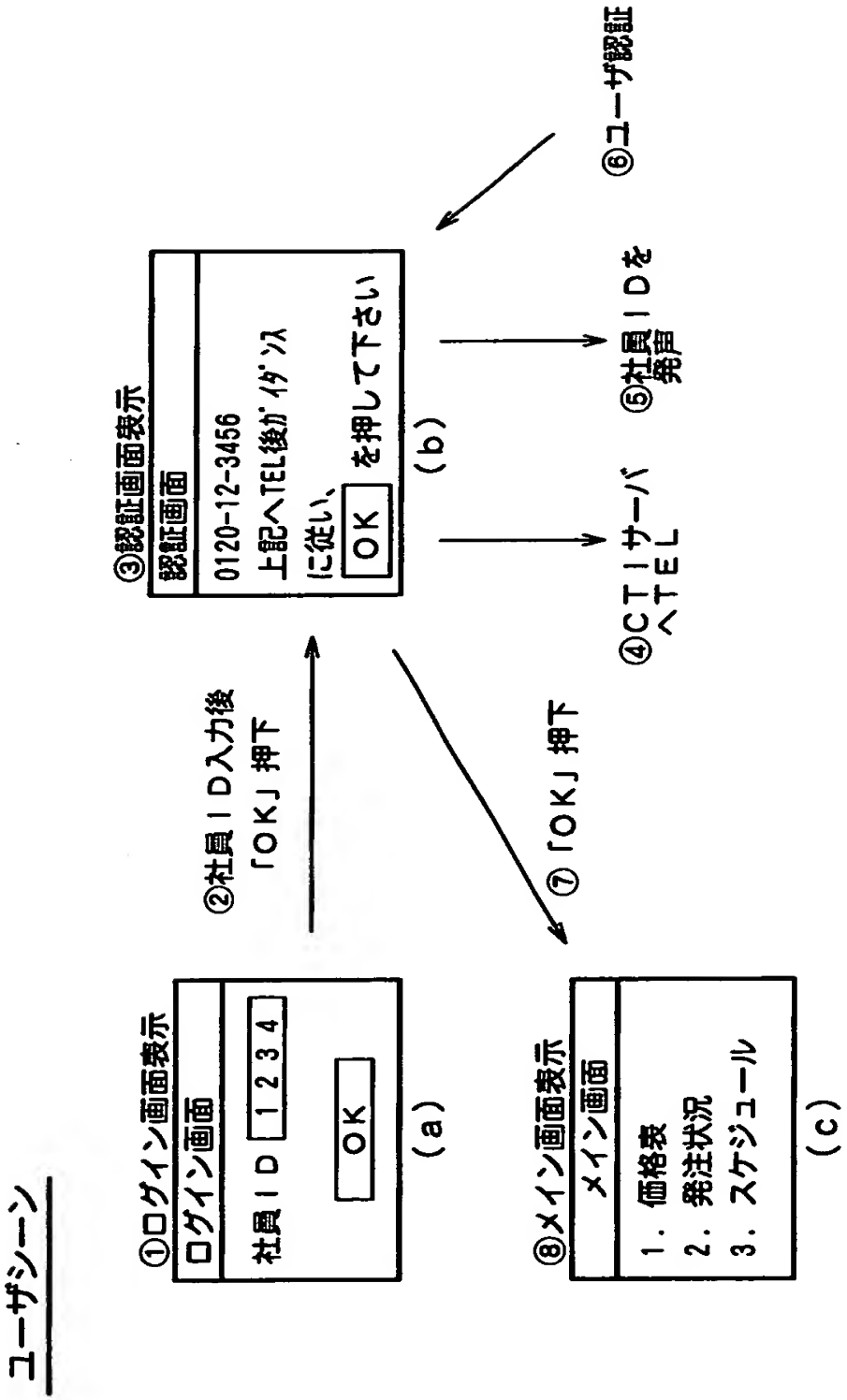
【図２】


開　始
ログイン画面を表示
S101
社員ＩＤを受付
S102
S103
ユーザ認証
データベースに受け付けた
社員IDが有る？
N
Y
ワンタイムＩＤを生成
S104
ログイン不可状態にして
ワンタイムＩＤを登録
S105
当該社員ＩＤによる
ログインを不可の
状態に変更
S106
認証画面を表示
S107
S108
キー入力
電話番号
S109
声紋照合処理
「OK」
S110
N
ワンタイムＩＤが
ログイン可能状態
Y
ワンタイムＩＤを削除
S111
メインメニューを表示
(ログイン)
S112
(処　理)
当該社員ＩＤによるログインを
可能な状態に変更
(ログアウト)
S113
終　了

【図３】


声紋照合処理
音声ガイダンスを送出
S201
音声認識処理により
入力された音声から
社員ＩＤ(コード）を取得
S202
S203
認証した社員ＩＤ
がユーザ認証データベースに登録
されている？
N
Y
声紋照合
S204
S205
本人と認証
N
Y
ワンタイムＩＤをログイン
可能な状態に変更
S206
照合結果通知後、
回線を切断
S207
終　了

【図４】


ユーザシーン
①ログイン画面表示
ログイン画面
社員ＩＤ 1234
OK
(a)
②社員ＩＤ入力後
「OK」押下
③認証画面表示
認証画面
0120-12-3456
上記へTEL後ガイダンス
に従い、
OK を押して下さい
(b)
④ＣＴＩサーバ
へＴＥＬ
⑤社員ＩＤを
発声
⑥ユーザ認証
⑦「OK」押下
⑧メイン画面表示
メイン画面
1．価格表
2．発注状況
3．スケジュール
(c)

【書類名】　　要約書

【要約】

【課題】　高いセキュリティ性を維持しつつユーザにかかる入力負荷を軽減させる。

【解決手段】　社員ＩＤに、当該ユーザが当該社員ＩＤを発声したときの声紋情報を対応付け格納したユーザ認証データベース９を設ける。Ｗｅｂサーバ４は、データ通信網３を介して携帯電話１から社員ＩＤを指定したログイン要求があると、ワンタイムＩＤをログイン不可状態で生成し、社員ＩＤに対応付けしてユーザ認証データベース９に登録すると共にワンタイムＩＤを携帯電話１へ返信する。ＣＴＩサーバ６は、電話回線網２を介した回線接続後、社員ＩＤをユーザに発声させ音声認識処理を行う。認証サーバ７は、音声認識された社員ＩＤに対応した声紋情報と発声された社員ＩＤとの声紋照合を行い、認証できたときにワンタイムＩＤをログイン可状態に変更する。携帯電話１は、ユーザ認証後ワンタイムＩＤをＣＴＩサーバ６へ送信して自動ログインする。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００６０１３〕

１．変更年月日　　１９９０年　８月２４日
［変更理由］　新規登録
住　所　東京都千代田区丸の内２丁目２番３号
氏　名　三菱電機株式会社